[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580023787.2

[43] 公开日 2007 年 8 月 15 日

[11] 公开号 CN 101019368A

[22] 申请日 2005.7.8
[21] 申请号 200580023787.2
[30] 优先权
[32] 2004.7.14 [33] US [31] 10/892,265
[86] 国际申请 PCT/US2005/024486 2005.7.8
[87] 国际公布 WO2006/025952 英 2006.3.9
[85] 进入国家阶段日期 2007.1.15
[71] 申请人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 E·布莱克尔 J·萨顿二世
C·霍尔 D·格劳罗克
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 顾嘉运

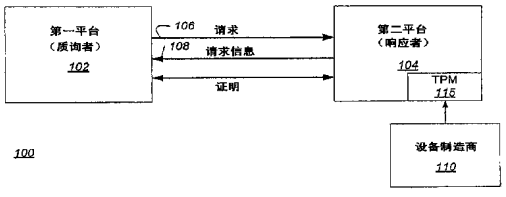
权利要求书 4 页 说明书 12 页 附图 9 页

[54] 发明名称

使用分发 CD 将直接证明私钥传递给设备的方法

[57] 摘要

现场将直接证明私钥传递给安装在客户计算机系统中的设备可按照安全方式完成而无需设备中的大量非易失性存储。唯一伪随机值在制造时生成并存储在设备中。该伪随机值用于生成对称密钥来对保存与设备相关联的直接私钥和私钥摘要的数据结构加密。所得的加密数据结构被存储在可移动存储介质(诸如 CD)上，并被分发给客户计算机系统的所有者。当设备在客户计算机系统上初始化时，系统检查系统中是否存在本地化的加密数据结构。如果否，则系统从可移动存储介质获取相关联的加密数据结构。设备使用从其所存储的伪随机值重新生成的对称密钥解密该加密数据结构，以获取直接证明私钥。如果该私钥有效，则它可用于客户计算机系统中该设备的随后的认证处理。



1．一种方法，包括：

生成与设备相关联的加密数据结构，所述加密数据结构包括私钥和私钥摘要；

基于伪随机生成的值为所述加密数据结构生成标识符；

将所述标识符和所述加密数据结构存储在可移动存储介质上；以及

将所述伪随机值存储到所述设备内的非易失性存储上。

2．如权利要求 1 所述的方法，其特征在于，还包括分发所述可移动存储介质和所述设备。

3．如权利要求 1 所述的方法，其特征在于，还包括为一类设备生成直接证明族密钥对。

4．如权利要求 3 所述的方法，其特征在于，所述私有密钥包括与所述直接证明族密钥对的公钥相关联的直接证明私钥，且还包括对所述直接证明私钥进行散列以生成所述私钥摘要。

5．如权利要求 1 所述的方法，其特征在于，还包括基于所述设备的伪随机值生成对称密钥。

6．如权利要求 5 所述的方法，其特征在于，所述生成标识符包括使用所述对称密钥加密数据值。

7．如权利要求 5 所述的方法，其特征在于，还包括使用所述对称密钥加密所述数据结构。

8．如权利要求 1 所述的方法，其特征在于，所述加密数据结构还包括随机初始化向量。

9．如权利要求 1 所述的方法，其特征在于，所述可移动存储介质包括 CD。

10．如权利要求 1 所述的方法，其特征在于，所述设备的伪随机值是唯一的。

11．一种制品，包括：含有多条机器可读指令的第一存储介质，其中当所述指令由处理器执行时，所述指令通过以下步骤允许向设备传递私钥：

生成与设备相关联的加密数据结构，所述加密数据结构包括私钥和私钥摘要；

基于伪随机生成的值为所述加密数据结构生成标识符；

将所述标识符和所述加密数据结构存储在第二可移动存储介质上；以及

将所述伪随机值存储到所述设备内的非易失性存储上。

12. 如权利要求 11 所述的制品，其特征在于，还包括用于为一类设备生成直接证明族密钥对的指令。

13. 如权利要求 12 所述的制品，其特征在于，所述私钥包括与所述直接证明族密钥对的公钥相关联的直接证明私钥，且还包括用于对所述直接证明私钥进行散列以生成所述私钥摘录的指令。

14. 如权利要求 11 所述的制品，其特征在于，还包括用于基于所述设备的所述伪随机值生成对称密钥的指令。

15. 如权利要求 14 所述的制品，其特征在于，所述用于生成标识符的指令包括用于使用所述对称密钥加密数据值的指令。

16. 如权利要求 14 所述的制品，其特征在于，还包括用于使用所述对称密钥加密所述数据结构的指令。

17. 如权利要求 11 所述的制品，其特征在于，所述加密数据结构还包括随机初始化向量。

18. 如权利要求 11 所述的制品，其特征在于，所述设备的所述伪随机值是唯一的。

19. 一种方法，包括：

确定包含私钥和私钥摘要且与安装在计算机系统中的设备相关联的加密数据结构是否被存储在所述计算机系统上的存储器中；

如果存储了所述加密数据结构，则禁用获取密钥命令的功能；以及

如果未存储所述加密数据结构，则从可由所述计算机系统访问的可移动存储介质中获取与所述设备相关联的所述加密数据结构，所述可移动存储介质存储加密数据结构的数据库。

20. 如权利要求 19 所述的方法，其特征在于，所述可移动存储介质包括由所述设备的制造商创建的 CD。

21. 如权利要求 19 所述的方法，其特征在于，所述获取加密数据结构包括，向所述设备发出所述获取密钥命令以启动私钥获取过程。

22. 如权利要求 19 所述的方法，其特征在于，所述私有密钥包括与一类设备的直接证明族密钥对的公钥相关联的直接证明私钥。

23. 如权利要求 21 所述的方法，其特征在于，所述私钥获取过程包括，基于所述设备中所存储的唯一伪随机值生成对称密钥。

24. 如权利要求 23 所述的方法，其特征在于，所述私钥获取过程包括基于所

述伪随机值为所述加密数据结构生成设备标识符。

25．如权利要求 24 所述的方法，其特征在于，所述私钥获取过程还包括，在所述可移动存储介质中搜索加密数据结构的数据库中由匹配所生成的设备标识符的标识符索引的条目，并将所述加密数据结构传送给所述设备。

26．如权利要求 25 所述的方法，其特征在于，所述私钥获取过程还包括，使用所述对称密钥解密从所述可移动存储介质接收的所述加密数据结构以获取所述私钥和所述私钥摘要。

27．如权利要求 26 所述的方法，其特征在于，所述私钥获取过程还包括，对所述私钥进行散列以生成新私钥摘要，将来自所解密的数据结构的私钥摘要与所述新私钥摘要进行比较，且当所述摘要匹配时接受所述私有密钥为对所述设备有效。

28．一种制品，包括：含有多条机器可读指令的第一存储介质，其中当所述指令由处理器执行时，所述指令通过以下步骤允许获取计算机系统中安装的设备的私钥

确定包含所述私钥和私钥摘要且与安装在所述计算机系统中的所述设备相关联的加密数据结构是否被存储在所述计算机系统上的存储器中；

如果存储了所述加密数据结构，则禁用获取密钥命令的功能；以及

如果未存储所述加密数据结构，则从可由所述计算机系统访问的可移动存储介质中获取与所述设备相关联的所述加密数据结构，所述可移动存储介质存储加密数据结构的数据库。

29．如权利要求 28 所述的制品，其特征在于，所述用于获取加密数据结构的指令包括用于向所述设备发出所述获取密钥命令以启动私钥获取过程的指令。

30．如权利要求 28 所述的制品，其特征在于，所述私钥包括与一类设备的直接证明族密钥对的公钥相关联的直接证明私钥。

31．如权利要求 29 所述的制品，其特征在于，所述私钥获取过程包括，用于基于所述设备中所存储的唯一伪随机值生成对称密钥的指令。

32．如权利要求 31 所述的制品，其特征在于，所述私钥获取过程包括用于基于所述伪随机值为所述加密数据结构生成设备标识符的指令。

33．如权利要求 32 所述的制品，其特征在于，所述私钥获取过程还包括，用于在所述可移动存储介质中搜索加密数据结构的数据库中由匹配所生成的设备标识符的标识符索引的条目并将所述加密数据结构传送给所述设备的指令。

34．如权利要求 33 所述的制品，其特征在于，所述私钥获取过程还包括，用

于使用所述对称密钥解密从所述可移动存储介质接收的所述加密数据结构以获取所述私钥和所述私钥摘要的指令。

35．如权利要求34所述的制品，其特征在于，所述私钥获取过程还包括，用于对所述私钥进行散列以生成新私钥摘要，将来自所解密的数据结构的私钥摘要与所述新私钥摘要进行比较，且当所述摘要匹配时接受所述私钥为对所述设备有效的指令。

36．一种方法，包括：

从计算机系统的存储器上检索包括私钥和私钥摘要且与所述计算机系统中所安装的设备相关联加密数据结构；

基于所述设备中所存储的唯一伪随机值生成对称密钥；

使用所述对称密钥解密所述加密数据结构以获取所述私钥和所述私钥摘要；

对所述私钥进行散列以生成新私钥摘要，将来自所解密的数据结构的所述私钥摘要与所述新私钥摘要进行比较；以及

当所述摘要匹配时接受所述私钥为对所述设备有效。

37．如权利要求36所述的方法，其特征在于，所述私钥包括与一类设备的直接证明族密钥对的公钥相关联的直接证明私钥。

38．如权利要求36所述的方法，其特征在于，所述设备包括所述计算机系统的外围设备。

39．如权利要求36所述的方法，其特征在于，还包括：

生成随机初始化向量；

通过使用所述对称密钥加密所述私钥、私钥摘要和随机初始化向量生成新的加密数据结构；以及

将所述新的加密数据结构存储到所述计算机系统的存储器中。

使用分发 CD 将直接证明私钥传递给设备的方法

背景

1．领域

本发明一般涉及计算机安全，尤其涉及安全地将密码密钥分发给处理系统中的设备。

2．描述

某些处理系统体系结构支持的内容保护和/或计算机安全特征要求，即特别受保护或“可信”的软件模块能够创建与处理系统中特定受保护或“可信”的硬件设备（诸如，例如图形控制器卡）的经认证的加密的通信会话。用于标识设备同时建立加密的通信会话的一种常用的方法是使用单边认证的 Diffie-Helman（DH）密钥交换处理。在这种处理中，设备被分配唯一的公共/私有 Rivest、Shamir 和 Adelman（RSA）算法密钥对或唯一的椭圆曲线密码（ECC）密钥对。然而，因为这种认证处理使用 RSA 或 ECC 密钥，因此设备具有唯一且可证实的身份，而这可能引起私密性问题。在最坏的情况中，这些问题可能导致缺乏原始设备制造商（OEM）对构建提供这种安全性的可信设备的支持。

附图简述

通过阅读本发明的以下详细描述，本发明的特征和优点将变得显而易见，附图中：

图 1 示出了以使用根据本发明的一个实施例操作的可信平台模块（TPM）实现的平台为特征的系统；

图 2 示出了包括图 1 的 TPM 的平台的第一实施例。

图 3 示出了包括图 1 的 TPM 的平台的第二实施例。

图 4 示出了以图 2 的 TPM 实现的计算机系统的示例性实施例。

图 5 是根据本发明的一个实施例的用于分发直接证明密钥的系统的示意图。

图 6 是示出根据本发明的一个实施例的分发直接证明密钥的方法的各阶段的

流程图。

图 7 是示出根据本发明的一个实施例的设备制造设置处理的流程图。

图 8 是示出根据本发明的一个实施例的设备制造生产处理的流程图。

图 9 是根据本发明的一个实施例的客户计算机系统设置处理的流程图。

图 10 是根据本发明的一个实施例的客户计算机系统处理的流程图。

详细描述

使用基于直接证明的 Diffie-Helman 密钥交换协议来允许受保护/可信的设备来认证自己并建立与可信的软件模块的加密通信会话，这避免在处理系统中创建任何唯一身份信息，从而避免引入私密性问题。然而，在生产线上的设备中直接嵌入直接证明私钥比其它方法需要设备上的更多受保护的非易失性存储，从而增加了设备的成本。本发明的一个实施例是允许直接证明私有密钥（例如，用于签署）以安全的方式在分发光盘只读存储器（CD-ROM）上传递并随后由设备自己安装在设备中的方法。本发明中提供的方法被设计成使得设备不必为安装过程揭示身份信息。在一个实施例中，支持这种能力所需的设备存储可能从大约 300-700 字节减少到大约 20 字节。对设备实现基于直接证明的 Diffie-Helman 密钥交换所需的非易失性存储的数量上的这一减少可使得这种技术能被更广泛地采用。

本说明书中对本发明的“一个实施例”或“实施例”的引用意味着，结合该实施例描述的特定特征、结构或特性被包括在本发明的至少一个实施例中。因此，在说明书各处出现的短语“在一个实施例中”的出现不必全部指的是同一实施例。

在以下描述中，某些术语用于描述本发明的一个或多个实施例的某些特征。例如，“平台”被定义为适用于发送和接收信息的任何类型的通信设备。各种平台的示例包括，但不限于或约束于计算机系统、个人数字助理、手机、机顶盒、传真机、打印机、调制解调器、路由器等。“通信链路”被宽泛地定义为适用于平台的一个或多个信息承载介质。各种类型的通信链路的示例包括但不限于或约束于电线、光纤、电缆、总线迹线或无线信号发送技术。

“质询者”指的是向另一实体请求某种真实性或权限的验证的任何实体（例如，个人、平台、系统、软件和/或设备）。正常地，这是在公开或提供所请求的信息之前执行的。“响应者”指的是被请求提供对其权限、有效性和/或身份的某种证明的任何实体。“设备制造商”可与“证书制造商”互换使用，它指的是制造或配置平台或设备的任何实体。

如此处所使用的，向质询者“证实”或“使之确信”响应者拥有或了解某些密码信息（例如，数字签名、诸如密钥等秘密等）意味着，基于向质询者公开的信息和证明，响应者具有该密码信息的可能性很高。向质询者对此进行证实而不向质询者“揭示”或“公开”该密码信息意味着，基于对质询者所公开的信息，质询者在计算上无法确定密码信息。

这样的证明在后文中被称为直接证明。术语“直接证明”指的是零知识证明，因为这些类型的证明在本领域中是公知的。具体地，如此处所引用的特定直接证明协议是于 11/27/2002 提交的转让给本发明的所有者的名为“System and Method for Establishing Trust Without Revealing Identity（用于建立信任而不揭示身份的系统和方法）”的共同待审专利申请第 10/306,336 号的主题。直接证明定义了其中发布者定义了共享如由发布者定义的公共特征的一族多个成员的协议。发布者生成将该族表示为一个整体的族公钥和私钥对（Fpub 和 Fpri）。使用 Fpri，发布者也可为族中的每一个别成员生成唯一的直接证明私有签署密钥（DPpri）。由个别 DPpri 签署的任何消息可使用族公钥 Fpub 来验证。然而，这样的验证仅标识该签署者是族中的成员；而不会暴露关于个别成员的任何唯一标识信息。在一个实施例中，发布者可以是设备制造商或代表。即，发布者可以是具有基于共享的特征定义设备族、生成族公钥/私钥对、以及创建 DP 私有密钥并将其注入设备中的能力的实体。发布者也可为族公钥生成标识密钥来源和设备族特征的证书。

现在参考图 1，示出了以根据本发明的一个实施例操作的可信硬件设备（被称为“可信平台模块”或“TPM”）实现的平台为特征的系统的一个实施例。第一平台 102（质询者）发送请求第二平台 104（响应者）提供关于其自身的信息的请求 106。响应于请求 106，第二平台 104 提供所请求的信息 108。

此外，为加强安全性，第一平台 102 可能需要验证所请求的信息 108 是来自由所选的一个或一组设备制造商（后文中称之为“设备制造商 110”）制造的设备。例如，在本发明的一个实施例中，第一平台 102 质询第二平台 104，要求它示出其具有由设备制造商 110 生成的密码信息（例如，签名）。质询可被包含在请求 106 内（如图所示）或作为单独的发送。第二平台 104 通过以回复的方式提供信息来回复该质询，以使第一平台 102 确信第二平台 104 具有由设备制造商 110 生成的密码信息而不揭示该密码信息。回复可以是所请求信息 108 的一部分（如图所示）或作为单独的发送。

在本发明的一个实施例中，第二平台 104 包括可信平台模块（TPM）115。TPM

115 是由设备制造商 110 制造的密码设备。在本发明的一个实施例中，TPM 115 包括含有密封在封装内的少量片上存储器的处理器。TPM 115 被配置成向第一平台 102 提供信息，该信息这可使其确定回复是从有效 TPM 发送的。所使用的信息是不会使 TPM 或第二平台的身份可能被确定的内容。

图 2 示出了具有 TPM 115 的第二平台 104 的第一实施例。对本发明的该实施例，第二平台 104 包括耦合至 TPM 115 的处理器 202。一般而言，处理器 202 是处理信息的设备。例如，在本发明的一个实施例中，处理器 202 可被实现为微处理器、数字信号处理器、微控制器或甚至状态机。或者，在本发明的另一实施例中，处理器 202 可被实现为可编程或硬编码的逻辑，诸如现场可编程门阵列（FPGA）、晶体管-晶体管逻辑（TTL）逻辑或甚至专用集成电路（ASIC）。

此处，第二平台 104 还包括存储单元 206 以允许存储密码信息，诸如以下的一个或多个：密钥、散列值、签名、证书等。“X”的散列值可被表示为“Hash(X)”。构想了如图 3 中所示，这样的信息可被存储在 TPM 115 的内部存储器 220 内以代替存储单元 206。密码信息可被加密，尤其当存储在 TPM 115 之外时。

图 4 示出了包括以图 2 的 TPM 115 实现的计算机系统 300 的平台的实施例。计算机系统 300 包括总线 302 和耦合至总线 302 的处理器 310。计算机系统 300 还包括主存储器单元 304 和静态存储器单元 306。

此处，主存储器单元 304 是用于存储信息和由处理器 310 执行的指令的易失性半导体存储器。主存储器 304 也可用于在处理器 310 执行指令期间存储临时变量或其它中间信息。静态存储器单元 306 是用于在更持久的特性上为处理器 310 存储信息和指令的非易失性半导体存储器。静态存储器 306 的示例包括，但不限于或约束于只读存储器（ROM）。主存储器单元 304 和静态存储器单元 306 均被耦合至总线 302。

在本发明的一个实施例中，计算机系统 300 还包括诸如磁盘或光盘等数据存储设备 308，其相应的驱动器也可被耦合至计算机系统 300 以便存储信息和指令。

计算机系统 300 也可经由总线 302 耦合至图形控制器设备 314，它控制诸如阴极射线管（CRT）、液晶显示器（LCD）或任何平面显示器等显示器（未示出），以便向最终用户显示信息。在一个实施例中，可期望图形控制器能够与正由处理器执行的软件模块建立经认证的加密通信会话。

一般，字母数字输入设备 316（例如键盘，小键盘等）可被耦合至总线 302 以便向处理器 310 传输信息和/或命令选择。另一类型的用户输入设备是光标控制

单元 318，诸如用于向处理器 310 传输方向信息和命令选择并用于控制显示器 314 上的光标移动的鼠标、跟踪球、触摸垫、指示笔、或光标方向键。

通信接口单元 320 也被耦合至总线 302。接口单元 320 的示例包括用于耦合至形成局域网或广域网的一部分的通信链路的调制解调器、网络接口卡或其它公知的接口。以此方式，计算机系统 300 可经由常规网络基础架构，诸如例如公司的内联网和/或因特网被耦合至多个客户机和/或服务器。

可以理解，某些实现可期望比上述更少或更多配备的计算机系统。从而，取决于各种因素，诸如价格约束、性能要求、技术改进和/或其它情况，对各种实现，计算机系统 300 的配置可以有所不同。

在至少一个实施例中，即使当计算机系统中存在其它敌对软件时，计算机系统 300 也可支持使用存储在主存储器 304 和/或大容量存储设备 308 中并正由处理器 310 执行的特别保护的“可信”软件模块（例如，防篡改软件或具有运行受保护程序的能力的系统）以便执行特定活动。这些可信软件模块中的某一些要求不仅对其它平台，而且也对同一平台内的一个或多个外围设备，诸如图形控制器 314 的同等“可信”的受保护访问。一般而言，这样的访问要求可信软件模块能够标识设备的能力和/或特定身份，然后与设备建立加密会话以允许不能被系统中的其它软件监听或哄骗的数据的交换。

标识设备并同时建立加密会话的一种现有技术的方法是使用单边认证的 Diffie-Hellman（DH）密钥交换处理。在这种处理中，设备被分配唯一的公共/私有 RSA 或 ECC 密钥对。设备持有并保护私钥，而公钥以及认证证书可被发布给软件模块。在 DH 密钥交换处理期间，设备使用其私钥签署消息，而软件模块可使用相应的公钥验证该消息。这允许软件模块认证消息的确来自所感兴趣的设备。

然而，因为这种认证处理使用 RSA 或 ECC 密钥，因此设备具有唯一且可证实的身份。可使设备以其私钥签署消息的任何软件模块可证实该特定唯一设备存在于计算机系统中。假定设备很少在处理系统之间迁移，则这也表示可证实的唯一计算机系统身份。此外，设备的公钥本身表示一恒定的唯一值；实际上是永久“cookie”。在某些情况中，这些特征可被认为是重要的私密性问题。

一种替换的方法在于 2004 年提交的转让给本申请的所有者的名为“An Apparatus and Method for Establishing an Authenticated Encrypted Session with a Device Without Exposing Privacy-Sensitive Information（用于与设备建立经认证的加密会话而不暴露私有性敏感的信息的装置和方法）”的共同待审的专利申请第

10/???,???号中描述。在这种方法中，以直接证明密钥代替在单边认证的Diffie-Helman处理中RSA或ECC密钥的使用。使用这种方法的设备可被认证为属于特定的一族设备，这可包括关于设备的行为或可信度的保证。该方法不暴露可用于建立表示该处理系统的唯一身份的任何唯一标识信息。

尽管这种方法工作良好，但它要求设备中的附加存储以保存直接证明私钥，这种密钥可能比RSA或ECC密钥大。为了减轻这种附加存储要求的负担，本发明的实施例定义用于当设备需要密钥时确保该设备具有直接证明私钥而无需设备中的实质上的附加存储的系统和过程。

在本发明的至少一个实施例中，设备制造商仅将128位的伪随机数存储到生产线中的设备内，大得多的直接证明私钥（DPpri）可被加密并使用分发CD来传递。其它的实施例可将长于或短于128位的数存储到设备内。这种处理确保仅有指定设备可解密并使用其分配的DPpri密钥。图5是根据本发明的一个实施例的用于分发直接证明密钥的系统500的示意图。这种系统中存在三个实体，即设备制造受保护系统502、设备制造生产系统503和客户计算机系统504。设备制造受保护系统包括用于设备506的制造之前的设置处理的处理系统。受保护系统502可由设备制造商操作，使得受保护系统针对来自设备制造位置以外（例如，它是封闭系统）的黑客的攻击受到保护。制造生产系统503可用于制造设备。在一个实施例中，受保护系统和生产系统可以是同一系统。设备506包括包含在客户计算机中的任何硬件设备（例如，存储器控制器、诸如图形控制器、I/O设备等外围设备等）。在本发明的实施例中，设备包括存储在设备的非易失性存储中的伪随机值RAND 508。

制造受保护系统包括受保护数据库510和生成功能512。受保护数据库包括用于存储由生成功能512按如下所述的方式生成的多个伪随机值（对每个要制造的设备至少有一个值）的数据结构。生成功能包括逻辑（以软件或硬件中任一种实现）以生成此处称为密钥块（keyblob）514的数据结构。密钥块514包括至少三个数据项。唯一直接证明私钥（DPpri）包括可由设备用来签署的密码密钥。DP私有摘要（digest）516（DPpri摘要包括根据诸如SHA-1等生成安全消息摘要的任何公知方法的DPpri的消息摘要。某些实施例可为兼容性的目的包括含有比特流的伪随机初始化向量（IV）518作为密钥块的一部分。如果为加密使用流密码，则IV用于在流密码中使用IV的公知方法。如果为加密使用块密码，则IV将被用作要加密的消息的一部分，因此使得加密的每一实例不同。

在本发明的实施例中，制造受保护系统生成一个或多个密钥块（如将在以下

详细描述）并将密钥块存储在 CD 522 上的密钥块数据库 520 中。在一个实施例中，在单个 CD 上可能有多个密钥块，唯一的限制是 CD 的物理存储限制。CD 然后经由典型的物理通道分发给计算机系统制造商、计算机分销商、消费者等。尽管 CD 此处被描述为存储介质，但可使用任何合适的可移动存储介质（例如，数字多功能盘（DVD）或其它介质）。

一旦 CD 被插入客户机计算机系统的 CDROM 驱动器（未示出）内之后，期望使用直接证明协议来进行认证以及与客户计算机系统 504 内所包含的设备 506 的通信会话的密钥交换的系统 504 可从 CD 上的密钥块数据库 520 读出所选密钥块 514。密钥块数据可由设备使用来生成本地化的密钥块（如下所述）供实现直接证明协议使用。设备驱动程序软件 526 由客户计算机系统执行来初始化并控制设备 506。

在本发明的实施例中，存在四个不同的操作阶段。图 6 是示出根据本发明的实施例的分发直接证明密钥的方法的各阶段的流程图 600。根据本发明的实施例，某些动作可在每一阶段执行。在设备制造商处，至少存在两个阶段：设置阶段 601 和制造生产阶段 604。设置阶段此处参考图 7 描述。制造生产阶段此处参考图 8 描述。在具有客户计算机系统的消费者处，至少存在两个阶段：设置阶段 606 和使用阶段 608。客户计算机系统设置阶段此处参考图 9 描述。客户计算机系统使用阶段此处参考图 10 描述。

图 7 是示出根据本发明的实施例的设备制造设置处理的流程图 700。在一个实施例中，设备制造商可使用制造受保护系统 502 执行这些动作。在框 702 处，设备制造商为要制造的每一类设备生成直接证明族密钥对（Fpub 和 Fpri）。每一唯一设备将具有一 DPpri 密钥，使得使用 DPpri 创建的签名可由 Fpub 验证。一类设备可包括任何设备的集合或子集，诸如所选生产线（即，设备类型）或基于版本号或设备的其它特征的生产线的子集。族密钥对由为其生成该密钥的一类设备使用。

对要制造的每一设备，制造受保护系统 502 的生成功能 512 执行框 704 到 720。首先，在框 704 处，生成功能生成唯一伪随机值（RAND）508。在一个实施例中，RAND 的长度为 128 位。在其它实施例中，可使用其它大小的值。在一个实施例中，多个设备的伪随机值可预先生成。在框 706 处，使用设备所支持的单向函数 f，生成功能从该唯一 RAND 值中生成对称加密密钥 SKEY（SKEY = f(RAND)）。该单向函数可以是适于该目的的任何已知算法（例如，SHA-1、MGF1、数据加密标准（DES）、三重 DES 等）。在框 708 处，在一个实施例中，生成功能通过使用

SKEY 加密“空条目”（例如，少量 0 字节）来生成将用于引用分发 CD 522 上该设备的密钥块 514 的标识符（ID）标签（设备 ID ＝ 使用 SKEY 加密（0..0））。在其它实施例中，可使用生成设备 ID 的其它方式，或可由 SKEY 加密其它值。

接着，在框 710 处，生成功能生成与设备的族公钥（Fpub）有关的 DP 私有签署密钥 DPpri。在框 713 处，生成功能使用已知方法（例如，使用 SHA-1 或另一散列算法）对 DPpri 进行散列以产生 DPpri 摘要。在框 714 处，生成功能为设备构建密钥块数据结构。密钥块包括至少 DPpri 和 DPpri 摘要。在一个实施例中，密钥块还包括具有多个伪随机生成的位的随机初始化向量。这些值可使用 SKEY 加密以产生加密的密钥块 514。在框 716 处，在框 708 处生成的设备 ID 和在框 714 处生成的加密的密钥块 514 可被存储在密钥块数据库 520 中的一条目中以便被发行给分发 CD 522。在一个实施例中，密钥块数据库中的条目可由设备 ID 指示。在框 718 处，当前的 RAND 值可被存储在受保护数据库 510 中。在框 720 处，可删除 SKEY 和 DPpri，因为它们将由设备在现场重新生成。可如此设计 DPpri 摘要的创建和由 SKEY 进行的随后的加密，使得 DPpri 的内容不能被不拥有 SKEY 的任何实体确定，且使得密钥块的内容在未经拥有 SKEY 的实体的随后检测的情况下不能被不拥有 SKEY 的实体修改。在其它实施例中，可使用用于提供这种秘密性和完整性保护的其它方法。在某些实施例中，可能不要求完整性保护，因此可使用仅提供秘密性的方法。在这种情况中，DPpri 摘要的值将不是必需的。

在框 720 之后的任何时候，在框 722 处，RAND 值的受保护数据库可被安全地上传到制造生产系统 503，它将在制造处理期间将 RAND 值存储到设备内。一旦验证了这种上传之后，RAND 值可从制造受保护系统 502 中安全删除。最后，在框 724 处，含有多个加密的密钥块的密钥块数据库可被“刻录”到公共分发 CD 522 上。在一个实施例中，CD 可沿着每一设备分发，如由设备 ID 字段所索引的，为每一设备使用一个密钥块数据库条目。此外，CD 包括密钥检索实用软件模块，它的使用将在以下更详细描述。

图 8 是示出根据本发明的实施例的设备制造生产处理的流程图 800。当设备在生产线中被制造时，在框 802 处，制造生产系统从受保护数据库中选择未使用的 RAND 值。所选 RAND 值然后可被存储到设备中的非易失性存储内。在一个实施例中，该非易失性存储包括 TPM。在框 804 处，一旦对 RAND 值的存储成功之后，制造生产系统毁去受保护数据库中该设备的 RAND 值的任何记录。此时，RAND 值的唯一副本被存储在设备中。

在一个替换实施例中，RAND 值可在设备的制造期间创建，然后被发送给制造受保护系统以便计算密钥块。

在另一实施例中，RAND 值可在设备上创建，且设备和制造受保护系统可订立使用不在设备外揭示 DPpri 密钥的方法生成 DPpri 密钥的协议。然后设备可创建设备 ID、SKEY 和密钥块。设备可将设备 ID 和密钥块传递给制造系统以便存储在受保护数据库 510 中。以这种方法，制造系统以受保护数据库中的相同信息（设备 ID、密钥块）结束，而不了解 RAND 或 DPpri 的值。

图 9 是根据本发明的一个实施例的客户计算机系统设置处理的流程图 900。客户计算机系统可执行这些动作作为引导系统的一部分。在框 902 处，客户计算机系统可按正常方式引导，设备的设备驱动程序 526 可被加载到主存储器内。当设备驱动程序被初始化并开始执行时，设备驱动程序确定在设备 506 的大容量存储设备 308 中是否已经存储了加密的本地化密钥块 524。如果是，则无需执行进一步的设置处理，且设置处理在框 906 处结束。如果否，则处理继续至框 908。在框 908 处，设备驱动程序引起消息对客户计算机系统的用户的显示，要求插入分发 CD 522。一旦 CD 被计算机系统读取之后，设备驱动程序然后启动 CD 上存储的密钥检索实用软件（图 5 中未示出）。该实用软件向设备 506 发出获取密钥命令以启动设备的 DP 私钥获取过程。

作为响应，在框 910 处，设备使用其单向函数 f 来从嵌入的 RAND 值 508 重新生成对称密钥 SKEY（现在供解密使用）（SKEY = f(RAND)）。在框 912 处，设备然后通过使用 SKEY 来加密“空条目”（例如，少量的 0 字节）来生成其唯一的设备 ID 标签（设备 ID ＝ 使用 SKEY 加密（0..0））。设备然后将设备 ID 返回给密钥检索实用软件。在框 914 处，密钥检索实用软件在 CD 上的密钥块数据库 520 中搜索包含匹配的设备 ID 的数据库条目，提取设备的加密密钥块，并将密钥块传送给设备。

在一个实施例中，如果在设备具有密钥块之后流氓软件试图向设备发送获取密钥命令，则设备不会以设备 ID 响应该流氓软件。相反，设备将返回出错指示符。实际上，如果设备访问了本地化的密钥块，则禁用获取密钥命令的功能。以这种方式，除非设备不含有密钥块，否则它不会揭示唯一设备 ID。

在框 916 处，设备使用对称密钥 SKEY 解密加密的密钥块，以产生 DPpri 和 DPpri 摘要，并将这些值存储到其非易失性存储中（解密的密钥块＝使用 SKEY 解密（IV、DPpri、DPpri 摘要））。可丢弃初始化向量（IV）。在框 918 处，设备

然后通过对DPpri进行散列并将结果与DPpri摘要进行比较来检查DPpri的完整性。如果比较结果良好，则设备接受DPpri作为其有效密钥。设备也可将密钥已获取标志置为真，以指示成功地获取了DP私钥。在框920处，设备选择一新IV并使用该新IV来创建新的加密的本地化密钥块（本地化密钥块＝使用SKEY加密（IV2、DPpri、DPpri摘要））。该新的加密的本地化密钥块可被返回给密钥检索实用软件。在框922处，密钥检索实用软件将加密的本地化密钥块存储到客户计算机系统内的存储中（诸如，例如大容量存储设备308）。设备的DPpri现在安全地存储在客户计算机系统中。

一旦设备在设置处理期间获取了DPpri之后，设备则可使用DPpri。图10是根据本发明的一个实施例的客户计算机系统处理的流程图。客户计算机系统可在设置完成之后的任何时候执行这些动作。在框1002处，客户计算机系统可按正常方式引导，设备的设备驱动程序526可被加载到主存储器内。当设备驱动程序被初始化并开始执行时，设备驱动程序确定在设备506的大容量存储设备308中是否已经存储了加密的本地化密钥块524。如果否，则执行图9的设置处理。如果存在该设备可用的加密的本地化密钥块，则处理继续至框1006。在框1006处，设备驱动程序检索加密的本地化密钥块，并将密钥块传送给设备。在一个实施例中，密钥块的传送可通过执行加载密钥块命令完成的。

在框1008处，设备使用其单向函数f从嵌入的RAND值508重新生成对称密钥SKEY（现在供解密使用）（SKEY = f(RAND)）。在框1010处，设备通过使用对称密钥SKEY来解密加密的本地化密钥块，以产生DPpri和DPpri摘要，并将这些值存储到其非易失性存储中（解密的密钥块＝使用SKEY解密（IV2、DPpri、DPpri摘要））。可丢弃第二初始化向量（IV2）。在框1012处，设备通过对DPpri进行散列并将结果与DPpri摘要进行比较来检查DPpri的完整性。如果比较结果良好（例如，摘要匹配），则设备接受该DPpri作为之前获取的有效密钥，并允许其使用。设备也可将密钥已获取标志置为真，以指示成功地获取了DP私钥。在框1014处，设备选择又一IV并使用该新IV创建新的加密的本地化的密钥块（本地化密钥块＝使用SKEY加密（IV3、DPpri、DPpri摘要））。该新的加密的本地化密钥块可被返回给密钥检索实用软件。在框1016处，密钥检索实用软件将加密的本地化密钥块存储到客户计算机系统内的存储中（诸如，例如大容量存储设备308）。设备的DPpri现在再次安全地存储在客户计算机系统中。

在本发明的一个实施例中，不必要一次生成所有的设备DP私钥。假定分发

CD 定期更新，则设备 DP 私钥可按需要按批生成。每次“刻录”分发 CD 时，它将包含迄今生成的密钥块数据库，包括已经被生成但还未分配给设备的那些设备密钥。

尽管此处讨论的操作可被描述为连续的处理，但某些操作实际上可并行或并发执行。此外，在某些实施例中，操作的顺序可被重排，而不背离本发明的精神。

此处所述的技术不限于任何特定硬件或软件配置；它们可应用于任何计算或处理环境。各种技术可以用硬件、软件或两者的组合实现。这些技术可用在可编程机器上执行的程序来实现，这些机器诸如移动或固定计算机、个人数字助理、机顶盒、手机和寻呼机、以及其它电子设备，它们均包括处理器、可由处理器读取的存储介质（包括易失性和非易失性存储器和/或存储元件）、至少一个输入设备和一个或多个输出设备。程序代码应用于使用输入设备输入的数据以执行所述功能并生成输出信息。输出信息可应用于一个或多个输出设备。本领域中的普通技术人员可以理解，发明可使用各种计算机系统配置来实现，包括微处理器系统、小型机、大型机等。本发明也可在分布式计算环境中实现，其中任务可由经由通信网络链接的远程处理设备执行。

每一程序可使用高级过程语言或面向对象的程序设计语言来实现以便与处理系统通信。然而，如有需要，程序可使用汇编语言或机器语言来实现。在任何情况中，语言可被编译或解释。

程序指令可用于使以指令编程的通用或专用处理系统执行此处所述的操作。或者，操作可由包含用于执行操作的硬连线逻辑的特定硬件组件，或由已编程的计算机组件和自定义硬件组件的任何组合执行。此处所述的方法可作为程序产品来提供，程序产品可包括其上存储有可用于对处理系统或其它电子设备编程来执行该方法的指令的机器可读介质。如此处所使用的，术语“机器可读介质”应包括能够存储或编码指令序列以便由机器执行并使机器执行此处所述的任何一种方法的任何介质。术语“机器可读介质”从而应包括但不限于，固态存储器、光盘和磁盘、以及编码数据信号的载波。而且，本领域中，通常以一种或另一种形式（例如，程序、过程、进程、应用程序、模块、逻辑等）将软件说成是采取动作或导致结果。这样的表示仅是陈述处理系统对软件的执行使得处理器执行动作或产生结果的简写形式。

尽管参考说明性实施例描述了本发明，但本描述不旨在以限制的含义解释。说明性实施例的各种修改以及本发明的其它实施例对本发明所属的领域中的技术

人员而言是显而易见的，它们被认为位于本发明的精神和范围内。

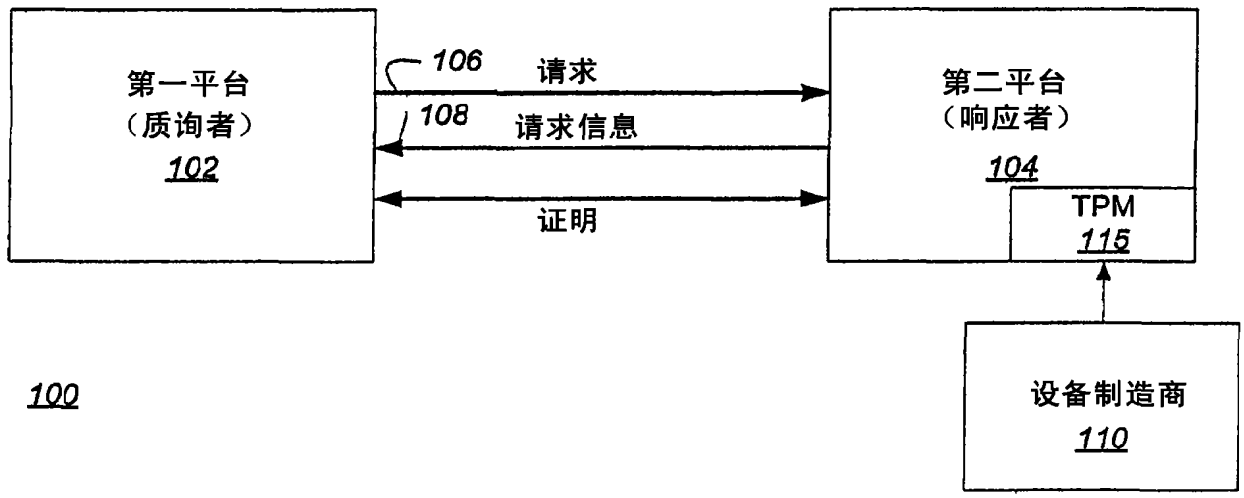

第一平台
（质询者）
102
106
请求
108
请求信息
证明
第二平台
（响应者）
104
TPM
115
设备制造商
110
100

图 1

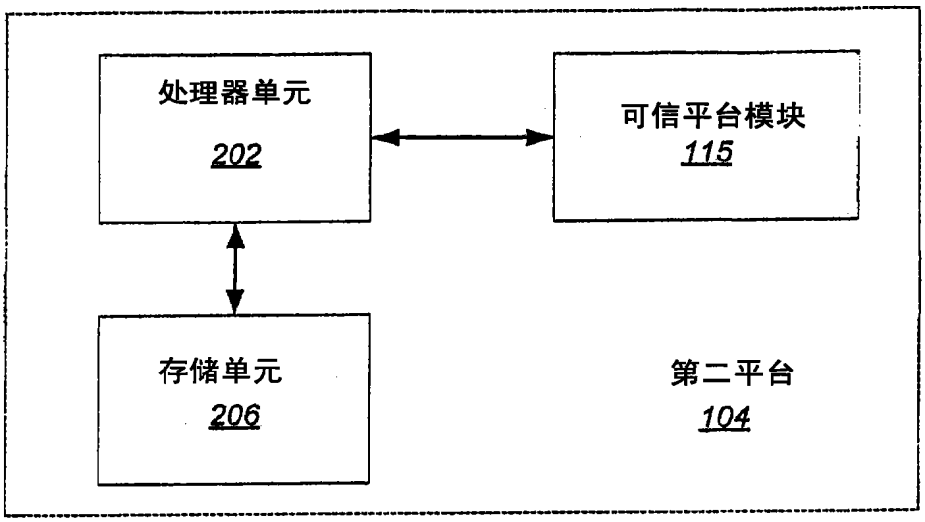

处理器单元
202
可信平台模块
115
存储单元
206
第二平台
104

图 2

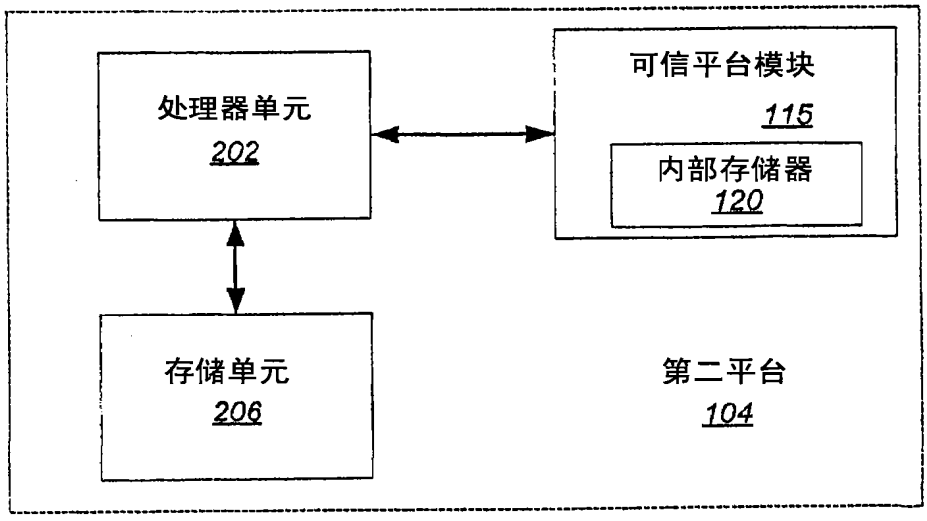

处理器单元
202
可信平台模块
115
内部存储器
120
存储单元
206
第二平台
104

图 3

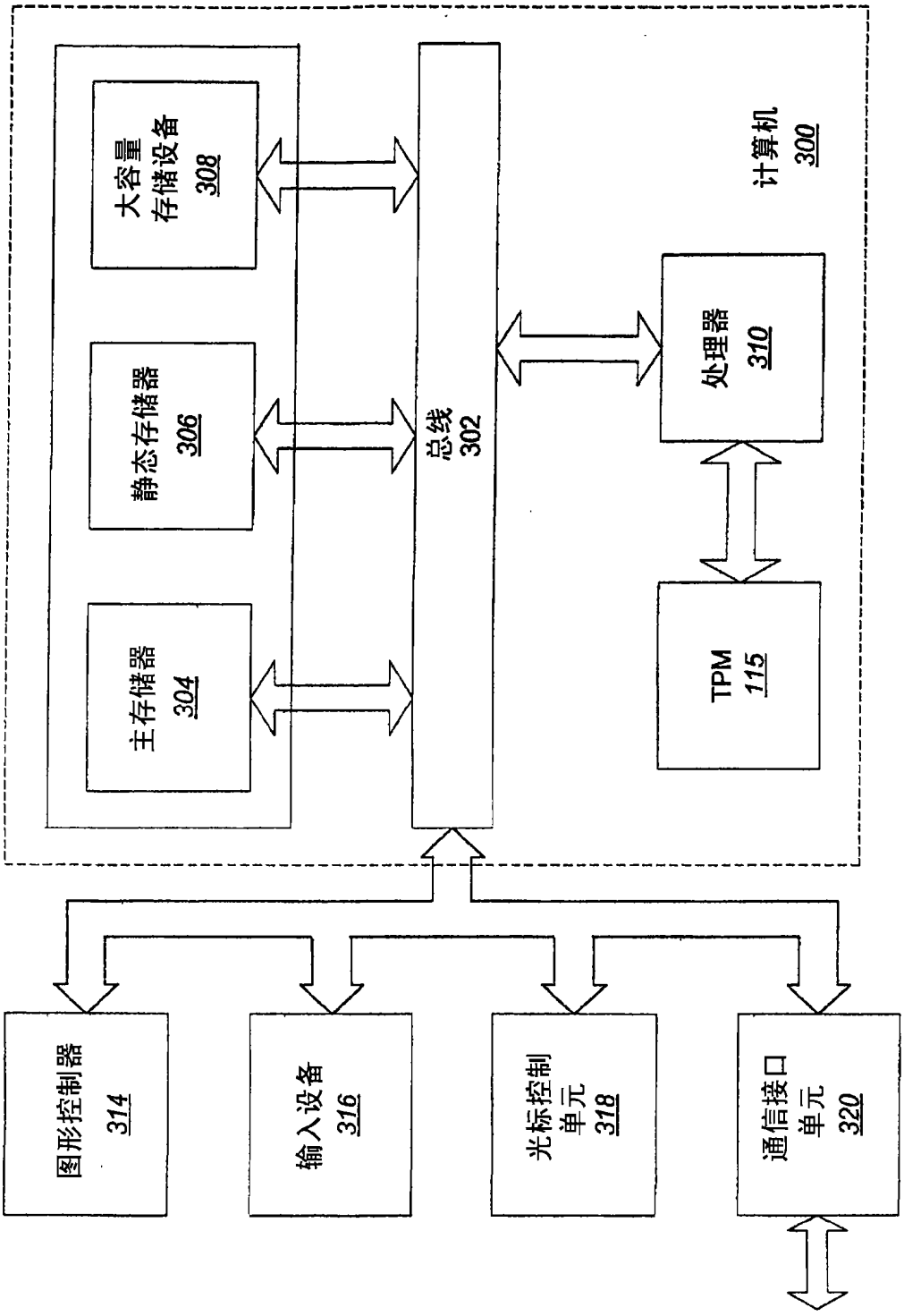

计算机
300
大容量
存储设备
308
静态存储器
306
主存储器
304
总线
302
处理器
310
TPM
115
104
图形控制器
314
输入设备
316
光标控制
单元
318
通信接口
单元
320

图 4

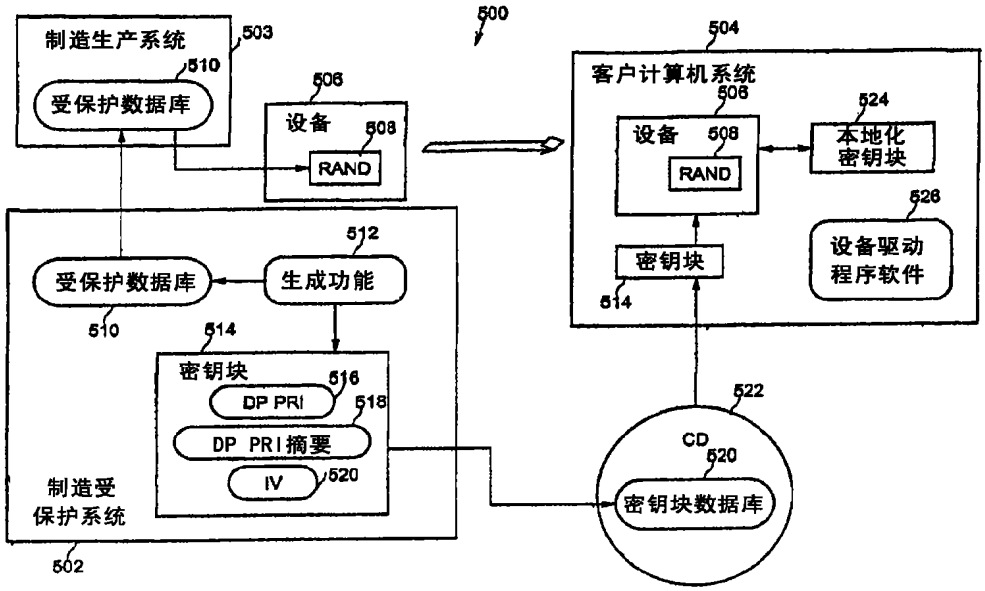

500
制造生产系统
503
510
受保护数据库
506
设备
508
RAND
504
客户计算机系统
506
设备
508
RAND
524
本地化
密钥块
526
设备驱动
程序软件
密钥块
514
512
受保护数据库
生成功能
510
514
密钥块
516
DP PRI
518
DP PRI摘要
IV
520
制造受
保护系统
502
522
CD
520
密钥块数据库

图 5

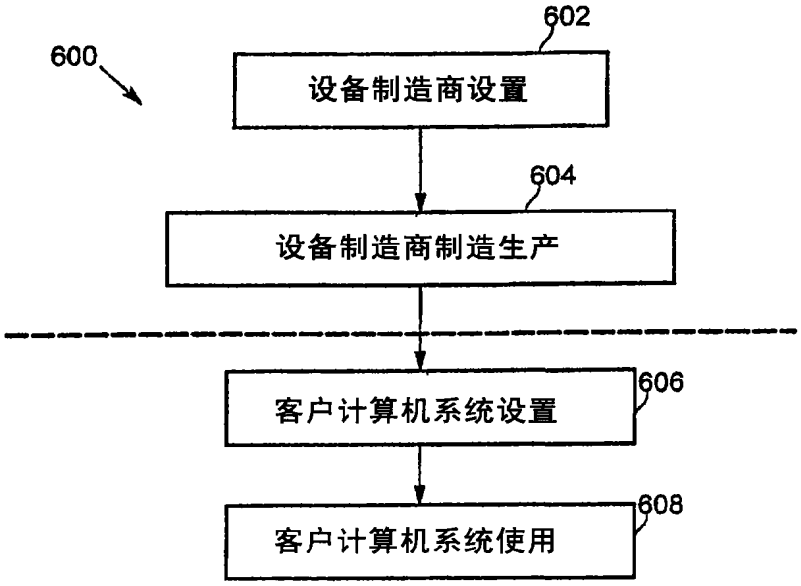


图 6

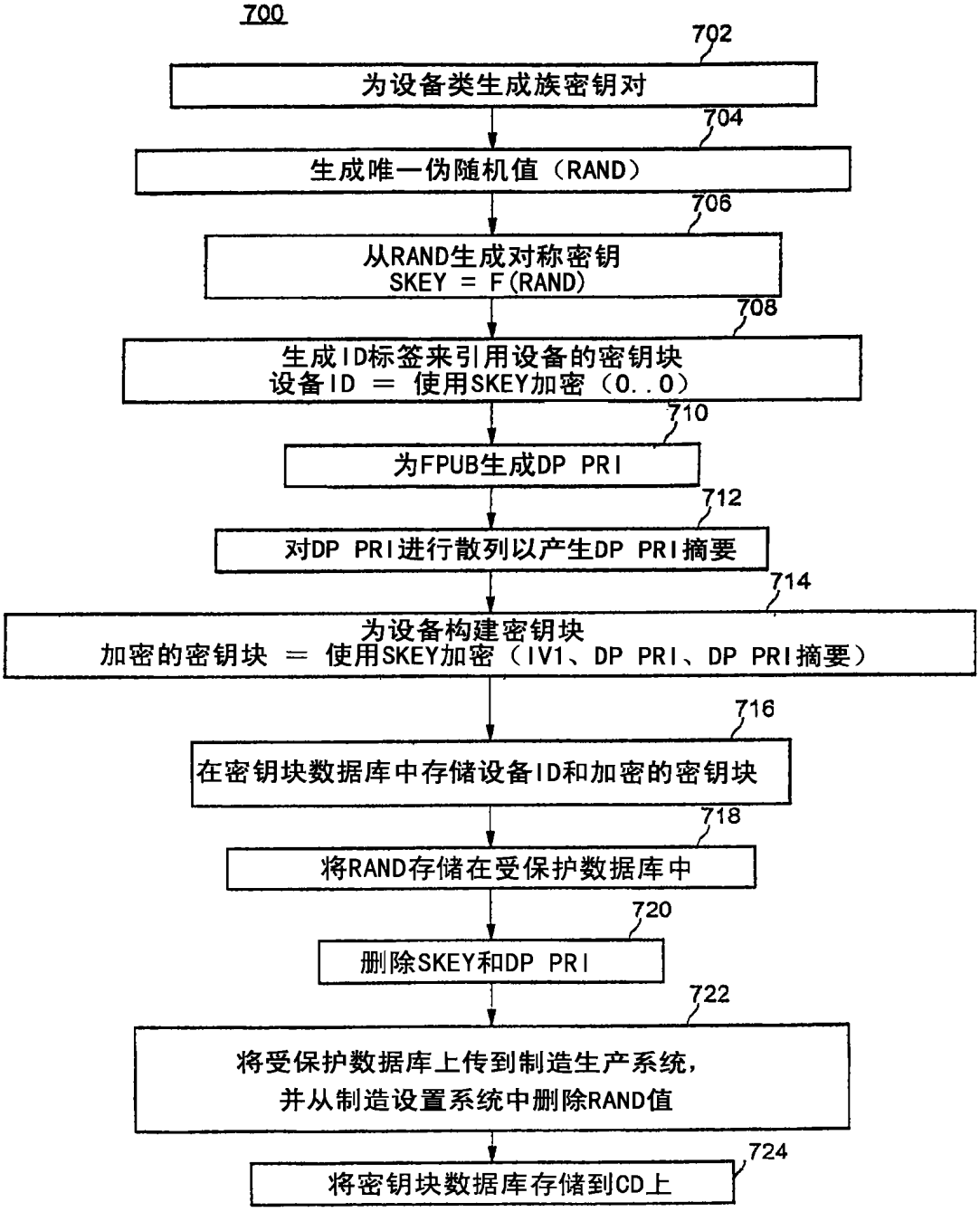

700
702
为设备类生成族密钥对
704
生成唯一伪随机值（RAND）
706
从RAND生成对称密钥
SKEY = F(RAND)
708
生成ID标签来引用设备的密钥块
设备ID = 使用SKEY加密（0..0）
710
为FPUB生成DP PRI
712
对DP PRI进行散列以产生DP PRI摘要
714
为设备构建密钥块
加密的密钥块 = 使用SKEY加密（IV1、DP PRI、DP PRI摘要）
716
在密钥块数据库中存储设备ID和加密的密钥块
718
将RAND存储在受保护数据库中
720
删除SKEY和DP PRI
722
将受保护数据库上传到制造生产系统，
并从制造设置系统中删除RAND值
724
将密钥块数据库存储到CD上

图 7

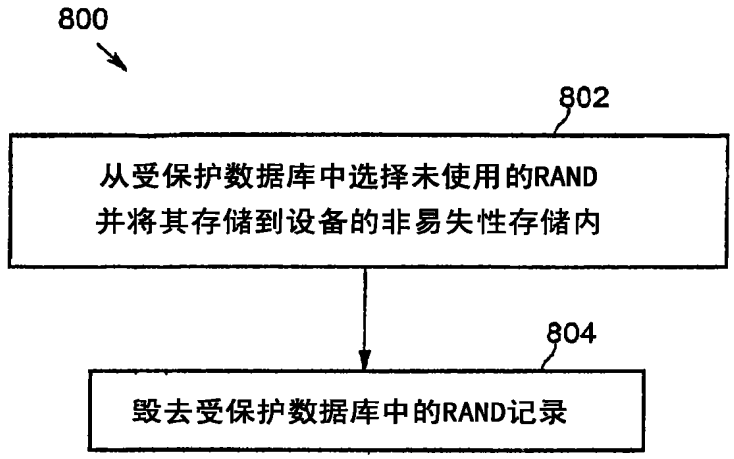

800
802
从受保护数据库中选择未使用的RAND
并将其存储到设备的非易失性存储内
804
毁去受保护数据库中的RAND记录

图 8

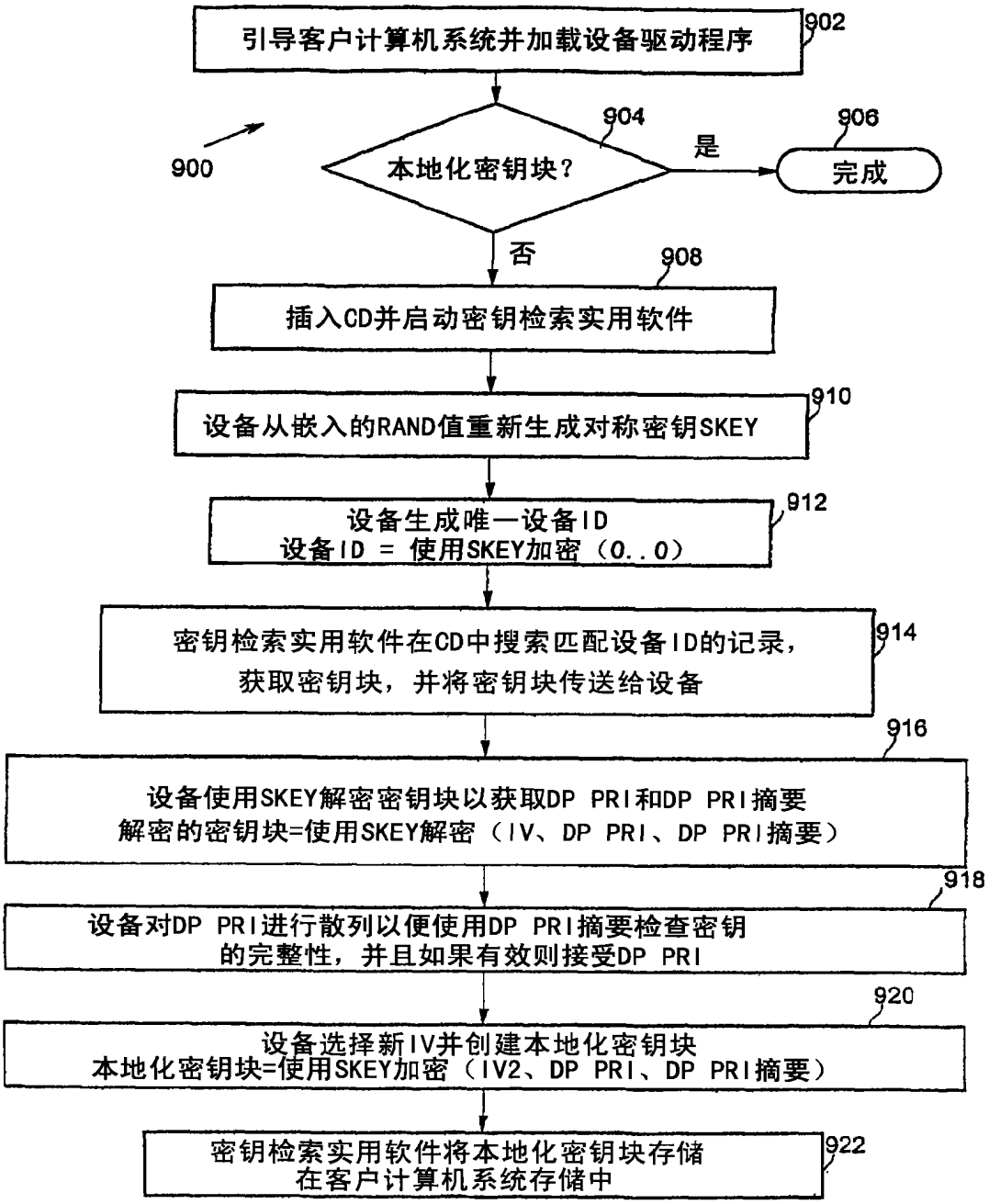

引导客户计算机系统并加载设备驱动程序
902
900
本地化密钥？
904
是
906
完成
否
908
插入CD并启动密钥检索实用软件
910
设备从嵌入的RAND值重新生成对称密钥SKEY
912
设备生成唯一设备ID
设备ID = 使用SKEY加密（0..0）
914
密钥检索实用软件在CD中搜索匹配设备ID的记录，
获取密钥块，并将密钥块传送给设备
916
设备使用SKEY解密密钥块以获取DP PRI和DP PRI摘要
解密的密钥块=使用SKEY解密（IV、DP PRI、DP PRI摘要）
918
设备对DP PRI进行散列以便使用DP PRI摘要检查密钥
的完整性，并且如果有效则接受DP PRI
920
设备选择新IV并创建本地化密钥块
本地化密钥块=使用SKEY加密（IV2、DP PRI、DP PRI摘要）
密钥检索实用软件将本地化密钥块存储
在客户计算机系统存储中
922

图 9

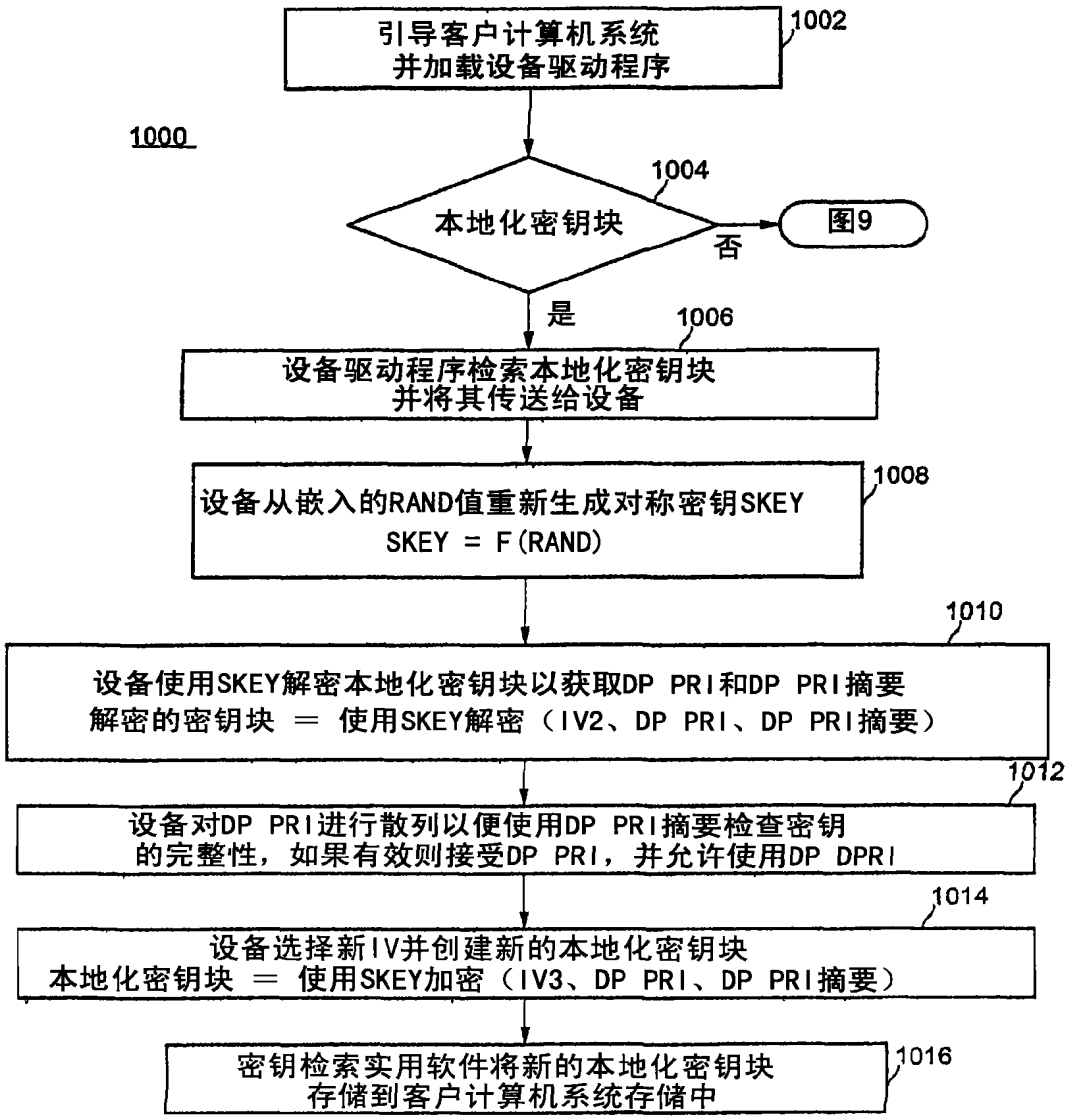

引导客户计算机系统
并加载设备驱动程序
1002
1000
1004
本地化密钥块
否
图9
是
1006
设备驱动程序检索本地化密钥块
并将其传送给设备
1008
设备从嵌入的RAND值重新生成对称密钥SKEY
SKEY = F(RAND)
1010
设备使用SKEY解密本地化密钥块以获取DP PRI和DP PRI摘要
解密的密钥块 = 使用SKEY解密（IV2、DP PRI、DP PRI摘要）
1012
设备对DP PRI进行散列以便使用DP PRI摘要检查密钥
的完整性，如果有效则接受DP PRI，并允许使用DP DPRI
1014
设备选择新IV并创建新的本地化密钥块
本地化密钥块 = 使用SKEY加密（IV3、DP PRI、DP PRI摘要）
密钥检索实用软件将新的本地化密钥块
存储到客户计算机系统存储中
1016

图 10